# MAXIMAL UNRAMIFIED 3-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS AND $\mathrm{SL}_2(\mathbb{Z}_3)$

L. BARTHOLDI AND M. R. BUSH

Abstract. The structure of the Galois group of the maximal unramified $p$-extension of an imaginary quadratic field is restricted in various ways. In this paper we construct a family of finite 3-groups satisfying these restrictions. We prove several results about this family and characterize them as finite extensions of certain quotients of a Sylow pro-3 subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$. We verify that the first group in the family does indeed arise as such a Galois group and provide a small amount of evidence that this may hold for the other members. If this were the case then it would imply that there is no upper bound on the possible lengths of a finite $p$-class tower.

## 1. Maximal unramified $p$-extensions and Schur-$\sigma$ groups

Let $k$ be an imaginary quadratic number field and $p$ be a prime. The $p$-class tower of $k$ is the sequence of fields

$$k = k_1 \subseteq k_2 \subseteq k_3 \subseteq \dots$$

where $k_{n+1}$ is the maximal unramified abelian $p$-extension of $k_n$. By Galois theory the fields $k_n$ correspond to the subgroups in the derived series of $G = \mathrm{Gal}\,(k^{nr,p}/k)$ where $k^{nr,p} = \bigcup_{n\geq 1} k_n$ is the maximal unramified $p$-extension of $k$. If we let $Cl_p(F)$ denote the $p$-Sylow subgroup of the class group of a number field $F$ then by class field theory $\mathrm{Gal}\,(k_{n+1}/k_n) \cong Cl_p(k_n)$ for $n \geq 1$. In particular $G/[G,G] \cong \mathrm{Gal}\,(k_2/k_1) \cong Cl_p(k)$ and so is finite.

Now assume also that $p \neq 2$. In [11] the notion of a Schur-$\sigma$ group is introduced. It encapsulates various properties that the Galois group $G$ is known to satisfy in this case. These are:

1. The generator rank and relation rank of $G$ (as a pro-$p$ group) are equal;
2. $G/[G,G]$ is finite;
3. There exists an automorphism $\sigma$ of order 2 on $G$ which induces the inverse automorphism $a \mapsto a^{-1}$ on $G/[G,G]$.

Several structural results are proved there about the presentations of such groups. One consequence of their work is that the extension $k^{nr,p}/k$ is finite only when the generator rank $d(G) \leq 2$. In particular all such extensions which are finite and non-abelian must have $d(G) = 2$.

---

*Date*: February 16, 2006.

1991 *Mathematics Subject Classification.* Primary : 11R37; Secondary : 11R32, 11R11, 20D15, 20F05, 20F14, 20G25.

The second author completed some of this work while he was a graduate student at the University of Illinois (Urbana-Champaign). Both authors would like to thank Nigel Boston for his many insights, suggestions and support.

In general it is exceedingly difficult to compute the Galois group $G$. For those examples in which the group is known to be finite the length of the derived series is usually small. Indeed to date the largest length observed is 3, see [5]. In the next section we will define a family of finite Schur-$\sigma$ groups and then show that the derived length for groups in this family is unbounded. In the last section we show that the first group in the family is isomorphic to $\mathrm{Gal}\,(k^{nr,p}/k)$ for several different choices of $k$.

## 2. A family of Schur $\sigma$-groups of unbounded derived length

Let $F$ be the free pro-3 group on two generators $x$ and $y$. Let $G_n$ be the Schur-$\sigma$ group defined by the pro-3 presentation

$$G_n = \langle x, y \mid r_n^{-1}\sigma(r_n),\, t^{-1}\sigma(t)\rangle$$

where $r_n = x^3 y^{-3^n}$, $t = yxyx^{-1}y$ and $\sigma : F \to F$ is the automorphism defined by $x \mapsto x^{-1}$ and $y \mapsto y^{-1}$. We will prove the following result.

**Theorem 2.1.** *For $n \geq 1$ the following hold:*

(i) *$G_n$ is a finite 3-group of order $3^{3n+2}$;*
(ii) *$G_n$ is nilpotent of class $2n+1$;*
(iii) *$G_n$ has derived length $\lfloor \log_2(3n+3) \rfloor$.*

The remainder of this section is devoted to the proof. We first define some auxiliary groups which are easier to study than $G_n$. Let $H_n$ be given by the pro-3 presentation

$$H_n = \langle x, y \mid x^3,\, y^{3^n},\, t^{-1}\sigma(t)\rangle,$$

and let $H$ be given by the pro-3 presentation

$$H = \langle x, y \mid x^3,\, t^{-1}\sigma(t)\rangle.$$

**Lemma 2.2.** *$G_n$ is a central cyclic extension of $H_n$; and all $H_n$'s are natural quotients of $H$.*

*Proof.* The first relation of $G_n$ is $x^6 = y^{2\cdot 3^n}$, so $x^6$ is central in $G_n$. Now the relator $x^6$ is equivalent to the relator $x^3$ in a 3-group; and the same argument holds for the relator $y^{3^n}$. It follows that the kernel of the natural map $G_n \to H_n$ is generated by $x^3$. The second assertion of the lemma is obvious. □

The next lemma exhibits an explicit, matrix representation of $H$. Let $\alpha \in \mathbb{Z}_3$ satisfy $\alpha^2 = -2$.

**Lemma 2.3.** *The map $\rho : H \to \mathrm{SL}_2(\mathbb{Z}_3)$, given by*

$$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad y \mapsto \alpha \begin{pmatrix} 0 & 1/2 \\ 1 & -1 \end{pmatrix},$$

*is an isomorphism between $H$ and a pro-3 Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$.*

We recall the recursive definition of the lower $p$-central series of a pro-$p$ group $G$: a series of closed subgroups of $G$

$$G = P_1(G) \geq P_2(G) \geq P_3(G) \geq \dots$$

defined by $P_k(G) = P_{k-1}(G)^p[G, P_{k-1}(G)]$ for each $k \geq 1$. Here the group on the right-hand side is the closed subgroup generated by all $p$-th powers of elements in $P_{k-1}(G)$, and commutators of elements from $G$ and $P_{k-1}(G)$.

*Proof.* We first claim that $\rho$ is a homomorphism. Let $\sigma' : \mathrm{SL}_2 \to \mathrm{SL}_2$ be conjugation by $\left(\begin{smallmatrix}-1 & 1\\ 0 & 1\end{smallmatrix}\right)$. It is then easy to check $\sigma'\rho = \rho\sigma$ and $\rho(x)^3 = \rho(t^{-1}\sigma(t)) = 1$

We will now show simultaneously that $\rho$ is injective, and that its image $P$ is a pro-3 Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$.

Consider the subgroup $K$ of index 3 in $H$ that is the normal closure of $yx^{-1}$. It is generated by $z_i = x^{-i}yx^{i-1}$, for $i \in \{0,1,2\}$. Its presentation, obtained by rewriting the presentation of $H$ with respect to the Schreier transversal $\{e, x, x^2\}$, is given by

$$K = \langle z_0, z_1, z_2 \mid z_i z_{i+1}^2 z_i^2 z_{i+1} \text{ for } i = 0,1,2\rangle.$$

The relators of $K$ may be written as $[z_i, z_{i+1}^{-1}]z_{i+1}^3 z_i^3$; therefore, inductively, every element of $[K,K]$ may be written as a cube ($K$ is said to be "powerful", see [6, 12, 13]). It follows that the lower central series $(\gamma_k(K))$ coincides with $(P_k(K))$ with $p = 3$. Then $\gamma_k(K)$ is generated, modulo $\gamma_{k+1}(K)$, by $\{z_i^{3^{k-1}}\}_{0 \le i \le 2}$. We conclude that $\gamma_k(K)/\gamma_{k+1}(K)$ has rank at most 3.

Recall that $\mathrm{SL}_2(\mathbb{Z}_3)$ has congruence kernels $N_k = 1 + 3^k M_2(\mathbb{Z}_3)$. The lower central series of $N_1$ is given by $\gamma_k(N_1) = N_k$, and the rank of $N_k/N_{k+1}$ is 3.

All the claims will follow if we show that $\{\rho(z_i^{3^{k-1}})\}$ spans $N_k/N_{k+1}$ for all $k \ge 1$; indeed then $\rho(K) = N_1$, and since the ranks along the lower central series of $K$ are bounded by 3, they must equal 3 and $\rho$ is then injective. We compute:

$$\rho(z_0^{3^{k-1}}) = \begin{pmatrix} \alpha^{-3^{k-1}} & 0 \\ 0 & \alpha^{3^{k-1}} \end{pmatrix};$$

and $\alpha^{3^{k-1}} \in 1 + 3^k\mathbb{Z}_3 \setminus 1 + 3^{k+1}\mathbb{Z}_3$; or, in other words, $\alpha$ is a topological generator of the torsion-free part of $\mathbb{Z}_3^\times$. Similarly,

$$\rho(z_1^{3^{k-1}}) = \begin{pmatrix} \alpha^{3^{k-1}} & \alpha^{-3^{k-1}} - \alpha^{3^{k-1}} \\ 0 & \alpha^{-3^{k-1}} \end{pmatrix},$$

$$\rho(z_2^{3^{k-1}}) = \begin{pmatrix} \alpha^{3^{k-1}} & 0 \\ \alpha^{-3^{k-1}} - \alpha^{3^{k-1}} & \alpha^{-3^{k-1}} \end{pmatrix},$$

and the off-diagonal entries are in $3^k\mathbb{Z}_3 \setminus 3^{k+1}\mathbb{Z}_3$.

We conclude by considering $P = N_1\langle\rho(x)\rangle$, which is a pro-3 Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$, and noting that $\rho(H) = P$ since they have isomorphic index-3 subgroups $K$ and $N_1$ respectively. □

**Remark 2.4.** (i) The proof is similar to a construction of presentations of congruence kernels in [1].

(ii) The following simple and general argument was generously communicated to us by Nigel Boston and Jordan Ellenberg, see [3]. Suppose $f : T \to U$ is a surjective homomorphism of pro-$p$ groups such that $H^1 f : H^1(U, \mathbb{F}_p) \to H^1(T, \mathbb{F}_p)$ is an isomorphism $H^2 f : H^2(U, \mathbb{F}_p) \to H^2(T, \mathbb{F}_p)$ is injective. Then $f$ is an isomorphism.

We may apply it to $T = K$ and $U = N_1$. It is not difficult to show that $f$ is surjective and that $H^1 f$ is an isomorphism. Now the cup product map $\bigwedge^2 H^1(U, \mathbb{F}_p) \to H^2(U, \mathbb{F}_p)$ is an isomorphism, because $U$ is uniform; so to prove injectivity of $H^2 f$ it suffices to show that $\bigwedge^2 H^1(T, \mathbb{F}_p) \to H^2(T, \mathbb{F}_p)$ is injective; this holds because $T/\Phi(\Phi(T))$ is abelian.

We may now identify $H_n$ with an appropriate quotient of $P$:

**Lemma 2.5.** *$H_n$ is the quotient of $P$ by the subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfying the congruences*

$$\begin{aligned} a, d &\equiv 1 \pmod{3^n} \\ b, c &\equiv 0 \pmod{3^n} \\ a + d &\equiv 2 \pmod{3^{n+2}} \\ a + b &\equiv 1 \pmod{3^{n+1}} \\ a + b - c &\equiv 1 \pmod{3^{n+2}} \end{aligned}$$

*Proof.* This amounts to computing the normal closure $R$ of $\rho(y^{3^n})$ in $P$. We have $y^3$ conjugate to $z_2 z_1 z_0$, which implies $\rho(y^{3^n}) \equiv \rho(z_0^{3^{n-1}} z_1^{3^{n-1}} z_2^{3^{n-1}})$ in $N_n/N_{n+1}$, and so the intersection of $R$ with $N_n/N_{n+1}$ is one-dimensional.

Then, taking commutators with $z_i$, we have $[y^3, z_i] \equiv z_{i-1}^{3^n} z_i^{3^n} / z_i^{3^n} z_{i+1}^{3^n} \equiv z_{i-1}^{3^n} / z_i^{3^n}$ in $N_{n+1}/N_{n+2}$; so the intersection of $R$ with $N_{n+1}/N_{n+2}$ is two-dimensional.

Finally, taking a commutator again, we have

$$[z_{i-1}^{3^n} / z_i^{3^n}, z_{i+1}] \equiv z_{i+1}^{-3^{n+1}}$$

in $N_{n+2}/N_{n+3}$, so the intersection of $R$ with $N_{n+2}/N_{n+3}$ is three-dimensional, and the same holds for $N_k/N_{k+1}$ for all $k \geq n+2$.

Writing the matrices $\rho(z_i^{3^n})$ then proves the lemma. □

Finally, we identify better the relation between $G_n$ and $H_n$:

**Lemma 2.6.** *The kernel of the natural map $G_n \to H_n$ is cyclic of order* 3.

*Proof.* The kernel is cyclic by Lemma 2.2. The order of $y^{3^n}$ in $G_n$ is at most 3, since $y^{3^n} = z_0^{3^{n-1}} z_1^{3^{n-1}} z_2^{3^{n-1}}$ and the relations in $H_n$ force cubes of $z_i^{3^{n-1}}$ to be commutators, and therefore to vanish in any central extension.

On the other hand, no relation in $G_n$ prevents $y^{3^n}$ from being non-trivial in $G_n$; therefore the order of $y$ is precisely $3^{n+1}$, and $|G_n| = 3|H_n|$. □

We are finally ready to prove the main theorem of this section:

*Proof of Theorem 2.1.* (i) We have $|G_n| = 3|H_n|$ by Lemma 2.6, and $|H_n| = 3^{3n+1}$ because the normal closure $R_n$ of $y^{3^n}$ in $H$ has index $3^{3n}$ in $N_1$, and therefore has index $3^{3n+1}$ in $P$.

(ii) We first compute the lower central series of $H_n$. It is obtained from that of $P$, as follows: $\gamma_1(P) = P$; and for $k \geq 1$, $\gamma_{2k}(P) = N_{k+1}\langle (z_0/z_1)^{3^k}, (z_1/z_2)^{3^k} \rangle$ and $\gamma_{2k+1}(P) = N_{k+1}\langle (z_0 z_1 z_2)^{3^k} \rangle$. The last index $k$ such that $R_n$ is not contained in $N_k$ is $n+1$, so the nilpotency class of $H_n$ is $2n+1$. Finally, the action by conjugation of $x$ on $y^{3^n} \equiv (z_0 z_1 z_2)^{3^{n-1}}$ is trivial, so the nilpotency class of $G_n$ is the same as that of $H_n$, namely $2n+1$; the last quotient $\gamma_{2n+1}(G_n)/\gamma_{2n+2}(G_n) = \langle x, y^{3^n} \rangle$.

(iii) The derived length of $G_n$ can also be obtained from the derived series of $P$: one has $P^{(2k)} = \gamma_{(2^{2k+2}-1)/3}(P)$ and $P^{(2k+1)} = \gamma_{(2^{2k+3}-2)/3}(P)$ using $[N_k, N_\ell] = N_{k+\ell}$, which comes from the identity

$$[1 + 3^m A, 1 + 3^n B] \equiv 1 + 3^{m+n}(AB - BA)$$

and the fact that the Lie algebra $sl_2$ is simple.

By (ii), we have $\gamma_{2n+1}(P) > R_n > \gamma_{2n+2}(P)$, so $P^{(k)} > R_n > P^{(k+1)}$ for $k = \lfloor \log_2(3n+3) \rfloor$. The same argument as above shows that the derived length of $G_n$ is equals that of $H_n$. □

**Remark 2.7.** The groups $G_n$ are finite 3-groups with the same number of relations as generators in their pro-3 presentations. It is an open question as to whether or not this implies that such groups must have an *abstract* presentation with equal numbers of generators and relations. Finite groups with this latter property are said to have *deficiency zero*. It is also open whether or not there exist abstract groups of deficiency zero with arbitrarily large derived length. To date the maximum length achieved is 6 (see [10]). If $G_n$ has deficiency zero then this question would be resolved.

We note that examples similar to ours have appeared in the literature before. In [1] a family of finite 3-generated $p$-groups (for odd prime $p$) with increasing nilpotency class and derived length is constructed. However our family of groups are the first 2-generated candidates to appear in the literature, as far as we know.

## 3. Explict computations of Gal $(k^{nr,3}/k)$

In [4] and [5] the $p$-group generation algorithm is used to compute the Galois groups of several $p$-extensions with restricted ramification. Here we use it to verify that $\mathrm{Gal}\,(k^{nr,3}/k) \cong G_1$ for several different imaginary quadratic fields $k$. For the reader's convenience we recall some definitions and give a brief description of the method.

Recall that $(P_k(G))$ denotes the lower $p$-central series of $G$. If $G$ is a finite $p$-group then this series is finite and the smallest $c$ such that $P_c(G) = \{1\}$ will be called the *$p$-class* of $G$. A $p$-group $H$ is called a *descendant* of $G$ if $H/P_c(H) \cong G$ where $c$ is the $p$-class of $G$. It is an *immediate descendant* if it has $p$-class $c+1$. The $p$-group generation algorithm [14] finds representatives (up to isomorphism) of all the immediate descendants of a given finite $p$-group $G$. Starting with the elementary abelian $p$-group on $d$ generators (for some fixed $d$) the algorithm allows one to compute a tree containing all finite $d$-generated $p$-groups. The $p$-class of a group determines the level of the tree in which it occurs.

For the Galois groups we are interested in we have additional information about the maximal abelian quotients of various subgroups of small index. This information is obtained by computing class groups of various extensions and applying the Artin reciprocity isomorphism from class field theory. This information is sometimes sufficient to eliminate all but finitely many groups from the tree of descendants described above, in which case we are left with a finite number candidates for the Galois group. A more precise formulation of the method and several examples in the case $p = 2$ can be found in [5].

In the case $p = 3$ we have obtained the following result using the symbolic computation package Magma [2]. (Note: we describe abelian groups by listing the orders of their cyclic components. So for instance $[3, 3]$ is the direct product of a cyclic group of order 3 with itself.)

**Proposition 3.1.** *Let $G$ be a pro-3 group and suppose $G/[G, G] \cong [3, 3]$, then $G$ has four closed subgroups of index 3. If these four subgroups have maximal abelian quotients $[3, 9]$, $[3, 9]$, $[3, 9]$ and $[3, 3, 3]$, then $G$ is a finite 3-group.*

In fact after starting the $p$-group generation algorithm on the 2-generated elementary abelian 3-group $[3, 3]$ with the restrictions described in the proposition

the computation terminates having found two candidates for $G$. These will be denoted by $Q_1$ and $Q_2$ and are generated by $\{x_i\}_{i=1}^5$ subject to the following power-commutator presentations.

$$(Q_1) \qquad \begin{aligned} x_1^3 &= x_4 & [x_2, x_1] &= x_3 \\ x_2^3 &= x_4 & [x_3, x_1] &= x_4 \\ & & [x_3, x_2] &= x_5 \end{aligned}$$

$$(Q_2) \qquad \begin{aligned} x_1^3 &= x_4^2 & [x_2, x_1] &= x_3 \\ & & [x_3, x_1] &= x_4 \\ & & [x_3, x_2] &= x_5 \end{aligned}$$

$Q_1$and $Q_2$ are the groups $(243, 5)$ and $(243, 6)$ respectively in Magma's or Gap's `SmallGroups` database [2, 7].

**Remark 3.2.** Note that in these power-commutator presentations if a power $x_r^3$ or commutator $[x_r, x_s]$ does not occur on the left-hand side of the given relations then it is assumed to be trivial.

**Corollary 3.3.** *All discriminants* $-50000 \le d \le 0$ *for which the field* $k = \mathbb{Q}(\sqrt{d})$ *has* $Gal(k^{nr,3}/k) \cong G_1$ *are contained in the following list:* $d = -4027$, $-8751$, $-19651$, $-21224$, $-22711$, $-24904$, $-26139$, $-28031$, $-28759$, $-34088$, $-36807$, $-40299$, $-40692$, $-41015$, $-42423$, $-43192$, $-44004$, $-45835$, $-46587$, $-48052$, $-49128$, *and* $-49812$.

*Proof.* For each of these fields $Cl_3(k) \cong [3, 3]$. Magma's class field theory package can be used to construct and verify that the four unramified extensions $\{k_i\}_{i=1}^4$ of degree 3 over $k$ have $Cl_3(k_i) \cong [3, 9]$ for three choices of $i$, and $Cl_3(k_i) \cong [3, 3, 3]$ for the remaining choice. By Proposition 3.1, $\mathrm{Gal}\,(k^{nr,3}/k)$ is isomorphic to $Q_1$ or $Q_2$. The group $Q_2$ has non-trivial Schur multiplier and hence can be eliminated (see [11]) leaving $Q_1$ as the only possibility. One can verify (by hand or by machine computation) that $G_1$ satisfies the conditions in Proposition 3.1. Hence we must also have $Q_1 \cong G_1$. □

**Remark 3.4.** Since $G_1$ has derived length 2 the fields described in the corollary all have 3-class towers of length 2. In [15] the field $\mathbb{Q}(\sqrt{-4027})$ is shown to have 3-class tower of length 2 by different means.

The following question remains to be answered:

**Question 3.5.** Is it possible, for all $n \ge 1$, to find an imaginary quadratic field $k$ such that $\mathrm{Gal}\,(k^{nr,3}/k) \cong G_n$?

If the answer is yes then this would imply that the lengths of finite $p$-class towers are unbounded. As a first step towards answering this question one might compute the abelian quotient invariants of the index 3 subgroups in $G_n$ for various $n \ge 2$, and then search for fields $k$ which have unramified extensions with matching 3-class groups. Using standard methods [8, 9] one can compute the abelian quotient invariants and it turns out that the result is independent of $n$. More precisely one obtains the following proposition.

**Proposition 3.6.** *For* $n \ge 2$ *the group* $G_n$ *has four subgroups of index* 3 *with abelian quotient invariants* $[3, 9]$, $[3, 3, 3]$, $[3, 3, 3]$, *and* $[3, 3, 3]$.

Moreover when one looks for examples of imaginary quadratic fields having unramified extensions with matching 3-class groups they seem relatively easy to find. The discriminants $d$ with $|d| < 50000$ for which there is a match are $d = -3896$, $-6583$, $-23428$, $-25447$, $-27355$, $-27991$, $-36276$, $-37219$, $-37540$, $-39819$, $-41063$, $-43827$, $-46551$.

At this point it becomes difficult to make further progress. Clearly one cannot use the abelian quotient invariants of the index 3 subgroups to separate out any of the groups $G_n$ for $n \geq 2$ as we did with $G_1$. If one restricts attention to the smallest groups $G_2$ and $G_3$ then differences in the abelian quotient invariants only show up when one looks at subgroups of index at least 27. The corresponding class group computations that one would need to carry out do not seem feasible currently.

## References


[1] I. V. Andožskiĭ, V. M. Cvetkov, A certain series of finite closed $p$-groups (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 278–290.

[2] W. Bosma, J. J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney (1996).

[3] N. Boston, J. Ellenberg, *Pro-p groups and towers of rational homology spheres*, accepted by Geometry and Topology.

[4] N. Boston, C. R. Leedham-Green, *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), 402–413.

[5] M. R. Bush, *Computation of the Galois groups associated to the* 2*-class towers of some quadratic fields*, J. Number Theory **100** (2003), 313–325.

[6] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups*, $2^{nd}$ edition, Cambridge University Press, 1999.

[7] GAP — Groups, Algorithms, and Programming, Version 4.4, *The GAP Group*, 2005. `http://www.gap-system.org`

[8] J. R. Howse, D. L. Johnson, *An algorithm for the second derived factor group*, in Groups - St. Andrews 1981, LMS lecture notes 71, Cambridge University Press 1982, 237–243.

[9] D. L. Johnson, *Presentations of Groups*, LMS Student Texts 15, Second Edition, Cambridge University Press, 1997.

[10] P. E. Kenne, *Some new efficient soluble groups*, Comm. Algebra **18** (1990), 2747–2753.

[11] H. Koch, B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Astérisque **24-25** (1975), 57–67.

[12] A. Lubotzky, A. Mann, *Powerful p-groups. I. Finite groups*, J. Algebra **105** (1987), no. 2, 484–505

[13] A. Lubotzky, A. Mann, *Powerful p-groups. II. p-adic analytic groups*, J. Algebra **105** (1987), no. 2, 506–515

[14] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Computation **9** (1990), no. 5–6, 677–698.

[15] A. Scholz, O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*, J. Reine Angew. Math. **171** (1934), 19–41.



École Polytechnique Fédérale de Lausanne (EPFL), Institut de Mathématiques B (IMB), CH-1015 Lausanne, Switzerland

*E-mail address*: `laurent.bartholdi@gmail.com`

Dept. of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA

*E-mail address*: `bush@math.umass.edu`